UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/930,384	08/15/2001	James E. King	5681-04200	9196

7590 04/21/2005

B. Noel Kivlin
Conley, Rose, & Tayon, P.C.
P.O. Box 398
Austin, TX 78767

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 04/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/930,384	KING ET AL.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *1-2*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 29-30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 29:

Claim 29 claims a microcontroller comprising a control program as recited in claim 21. Since claim 29 claims a microcontroller, the statutory class of invention as presently claimed is inconsistent with that of a control program which is the statutory class of its parent claim. Therefore, it is unclear whether the applicants intended for the claim to be rewritten in a form so that it is independent of the control program so that the microcontroller comprising that control program can be claimed properly.

As per claim 30:

Claim 30 claims a server computer. Since claim 30 claims a server computer, the statutory class of invention as presently claimed is inconsistent with that of a control program which is the statutory class of its parent claim. Therefore, it is unclear whether the applicants intended for the claim to be rewritten in a form so that it is independent of the control program so that the server computer comprising a device reader for reading a portable storage, etc. can be claimed properly.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-11, 13-15, and 17-36 are rejected under 35 U.S.C. 102(b) as being anticipated by Thomlinson et al (6,044,155).

As per claim 1:

Thomlinson teaches a network supervisory computer verifies that the user corresponding to the user identification has currently been authenticated at the local computer (col. 3, lines 21-23), the personal computer further includes a hard disk for reading from and writing to a hard disk and a magnetic disk drive for reading from or writing to a removable magnetic disk or optical disk (col. 6, lines 7-16) and a smart card storage provider might be installed to allow storage of core data items on a smart card (col. 8, lines 13-15), a personal computer including a processing unit where bus structures include a memory bus or memory controller (col. 5, lines 60-67) and the system memory includes read only memory input/output system (col. 6, lines 1-12), data secrets to be securely stored on the user's local computer where the core data secrets are encrypted on the user's computer with locally generated encryption key derived from a logon secret supplied by a user, in a network environment (col. 1, lines 6266), and the local key could be encrypted and stored on the computer which would involve another key (col. 2, lines 12-17).

As per claim 2:

Further, Thomlinson teaches a personal computer including a processing unit where bus structures include a memory bus or memory controller (col. 5, lines 60-67). The system memory is coupled to the processing unit (col. 5, line 65). This storage device is only controlled/coupled by/to the CPU, which regulates access, and no other device.

As per claim 3:

Further, Thomlinson teaches data secrets to be securely stored on the user's local computer where the core data secrets are encrypted on the user's computer with locally generated encryption key derived from a logon secret supplied by a user, in a network environment (col. 1, lines 62-66).

As per claim 4:

Further, Thomlinson teaches data secrets to be securely stored on the user's local computer where the core data secrets are encrypted on the user's computer with locally generated encryption key derived from a logon secret supplied by a user, in a network environment (col. 1, lines 62-66), in a network environment (col. 2, line 1).

As per claim 5:

Further, Thomlinson teaches a storage system holding data items such as financial information, trust profiles, etc. (col. 7, lines 25-32) where a file may be used to hold data items.

As per claim 6:

Further, Thomlinson teaches a storage system holding data items such as financial information, trust profiles, etc. (col. 7, lines 25-32) where a file may be used to hold data items.

As per claim 7:

Further, Thomlinson teaches encrypting the item key and the item authentication key with a master key where a key generation code is generated from an item key and item authentication key (col. 11, lines 36-47) triggered by a user's logon name & password, and storing & recovering data protection keys where a protected data item that is a local encryption key that is derived from a user-supplied password or other secret, performed by a computer or domain controller communicating between themselves using network technologies (col. 12, lines 47-51).

As per claim 8:

Further, Thomlinson teaches an encryption client key is sent to the network supervisory computer after performing the optional step of encrypting the client key where the supervisory computer recovers the client key (col. 13, lines 38-47). The encryption is meant to shroud the client key from the domain controller during subsequent steps (col. 13, lines 34-37).

As per claim 9:

Further, Thomlinson teaches the system memory includes RAM (col. 6, lines 1-3) where program modules may be stored including an operating system, program modules, program data, and application programs (col. 6, lines 29-32).

As per claim 10:

Further, Thomlinson teaches a system bus, which couples various system components including the system memory to the processing unit, and a memory controller, which is linked to a ROM and RAM (col. 5, lines 60-65 and col. 6, lines 1-7). A microcontroller consists of a controller and a processing unit.

As per claim 11:

Further, Thomlinson teaches items being stored in smart cards (col. 7, lines 36-41).

As per claim 13:

Thomlinson teaches a processing device linked through a communications network (col. 5, lines 55-59), a personal computer including a processing unit, a system memory, and a system bus (col. 5, lines 60-65), core data secrets stored on a computer which are encrypted with an encryption key derived from a logon secret (col. 1, lines 62-66) thus the storage holds an encryption key and a data secret identifying the processing unit, a local key encrypted with another key and stored on the local computer (col. 2, lines 12-17) where the key-key encryption is required prior to access to the storage, a network operating system authentication or logon where the password or code can be gathered from an authentication step (col. 11, lines 1-6) where the processing unit supplies the multi-keys as a code or password (col. 10, lines 65-67), and the encrypted items are retrieved from storage when requested by an authorized application program where a user key is decrypts the master key and master authentication key, which is used in conjunction with the specified MAC to verify that the master key is decrypted correctly, to decrypt an appropriate item key and corresponding item authentication key. The item authentication key is used in conjunction with the MAC to verify that the item key decrypted correctly. The item key decrypts the actual data item. (col. 11, lines 61-67 and col. 12, lines 1-5)

As per claim 14:

Further, Thomlinson teaches the logon of a user, from the logon password a master key is derived, and the core data secrets or other user data is encrypted with the master key (col. 13, lines 20-29). A processing unit will perform the encryption. Once, the encrypted core data secrets, which may be commands, are stored using the server (col. 13, lines 20-32).

As per claim 15:

Further, Thomlinson teaches items being stored in smart cards (col. 7, lines 36-41), a system bus, which couples various system components including the system memory to the processing unit, may be a memory controller, which is linked to a ROM and RAM (col. 5, lines 60-65 and col. 6, lines 1-3), and a smart card authentication provider may authenticate users by requiring them to insert their smart cards into a smart card reader (col. 8, lines 15-20).

As per claim 17:

Further, Thomlinson teaches remote procedure calls are made, under the direction of application programs which exploit the functionality of the calls, to read from a storage system (col. 8, lines 30-42).

As per claim 18:

Further, Thomlinson teaches a system bus, which couples various system components including the system memory to the processing unit, may be a memory controller, which is linked to a ROM and RAM (col. 5, lines 60-65 and col. 6, lines 1-3). A microcontroller consists of a controller and a processing unit.

As per claim 19:

Further, Thomlinson teaches the storage server performs authentication and verification procedures (col. 7, lines 50-53) which allows the server to act as a processing unit.

As per claim 20:

Further, Thomlinson teaches a server with well-defined interfaces (col. 2, lines 37-45). This server may be rack mountable to allow easy connection to a modem, the Internet, and other computers (col. 6, lines 47-67 and col. 7, lines 1-6).

As per claim 21:

Thomlinson teaches processing devices that perform tasks through computer-executable instructions linked through a communications network (col. 5, lines 57-59), a personal computer including a processing unit where bus structures include a memory bus or memory controller (col. 5, lines 60-67), data secrets to be securely stored on the user's local computer where the core data secrets are encrypted on the user's computer with locally generated encryption key derived from a logon secret supplied by a user, in a network environment (col. 1, lines 62-66), the local key could be encrypted and stored on the computer which would involve another key (col. 2, lines 1217), a network operating system authentication or logon where the password or code can be gathered from an authentication step (col. 11, lines 1-6) where the processing unit supplies the multi-keys as a code or password (col. 10, lines 65-67), and the encrypted items are retrieved from storage when requested by an authorized application program where a user key is decrypts the master key and master authentication key, which is used in conjunction with the specified MAC to verify that the master key is decrypted correctly, to decrypt an appropriate item key and corresponding item authentication key. The item authentication key is used in conjunction with the MAC to verify that the item key decrypted correctly. The item key decrypts the actual data item. (col. 11, lines 61-67 and col. 12, lines 1-5)

As per claim 22:

Further, Thomlinson teaches access to storage once a user-supplied code generates a user key, which encrypts the master key and master authentication key. The stored encrypted individual data item, the item authentication code, the encrypted item key, the encrypted item

authentication key, the key authentication code, the encrypted master key and the encrypted master authentication key (col. 11, lines 4460).

As per claim 23:

Further, Thomlinson teaches items being stored in smart cards (col. 7, lines 36-41), a system bus, which couples various system components including the system memory to the processing unit, may be a memory controller, which is linked to a ROM and RAM (col. 5, lines 60-65 and col. 6, lines 1-3), and a smart card authentication provider may authenticate users by requiring them to insert their smart cards into a smart card reader (col. 8, lines 15-20).

As per claim 24:

Further, Thomlinson teaches an item authentication code is generated using a MAC in conjunction with a randomly generated item authentication key (col. 11, lines 30-36).

As per claim 25:

Further, Thomlinson teaches operating systems use remote procedure calls to read a protected storage device (col. 8, lines 30-38) and each storage provider is adapted to securely store data using a specific type of media, such as smart cards (col. 2, lines 28-30).

As per claim 26:

Further, Thomlinson teaches a number of program modules may be stored on hard disk, magnetic disk, optical disk, including an operating system, one or more application programs (col. 6, lines 29-33).

As per claim 27:

Further, Thomlinson teaches a computer includes a processing unit (col. 5, lines 60-67) where program modules are stored. The storage is connected to the processing unit (col. 6, lines 29-35).

As per claim 28:

Further, Thomlinson teaches a system bus, which couples various system components including the system memory to the processing unit, may be a memory controller, which is linked to a ROM and RAM (col. 5, lines 60-65 and col. 6, lines 1-3).

As per claim 29:

Further, Thomlinson teaches an input/output system containing the basic routines that help to transfer information, a hard disk drive for reading and writing, and computer readable instructions (col. 5, lines 65-67 and col. 6, lines 1-20).

As per claim 30:

Further, Thomlinson teaches a personal computer including a processing unit where bus structures include a memory bus or memory controller (col. 5, lines 60-67), data secrets to be securely stored on the user's local computer where the core data secrets are encrypted on the user's computer with locally generated encryption key derived from a logon secret supplied by a user, in a network environment (col. 1, lines 62-66) and operating systems use remote procedure calls to read a protected storage device (col. 8, lines 30-38) and each storage provider is adapted to securely store data using a specific type of media, such as smart cards (col. 2, lines 28-30).

As per claim 31:

Further, Thomlinson teaches a processing device linked through a communications network (col. 5, lines 55-59), remote processing devices linked through a communications

network and containing remote memory storage devices (col. 5, lines 56-59), a personal computer includes a disk drive for reading from a hard disk (col. 6, lines 7-12), data secrets to be securely stored on the user's local computer where the core data secrets are encrypted on the user's computer with locally generated encryption key derived from a logon secret supplied by a user, in a network environment (col. 1, lines 62-66), and the local key could be encrypted and stored on the computer which would involve another key (col. 2, lines 12-17).

As per claim 32:

Further, Thomlinson teaches a personal computer including a processing unit where bus structures include a memory bus or memory controller (col. 5, lines 60-67).

As per claim 33:

Further, Thomlinson teaches data secrets to be securely stored on the user's local computer where the core data secrets are encrypted on the user's computer with locally generated encryption key derived from a logon secret supplied by a user, in a network environment (col. 1, lines 62-66).

As per claim 34:

Further, Thomlinson teaches data secrets to be securely stored on the user's local computer where the core data secrets are encrypted on the user's computer with locally generated encryption key derived from a logon secret supplied by a user, in a network environment (col. 1, lines 62-66), in a network environment (col. 2, line 1).

As per claim 35:

Further, Thomlinson teaches a network operating system authentication or logon where the password or code can be gathered from an authentication step (col. 11, lines 1-6) where the

processing unit supplies the multi-keys as a code or password (col. 10, lines 65-67), an item key and item authentication key are encrypted using a master key where the master key is used to generate a key authentication code so the correct decryption of the item key and item authentication key can be verified later (col. 11, lines 14-21), an encryption client key is sent to the network supervisory computer after performing the optional step of encrypting the client key where the supervisory computer recovers the client key (col. 13, lines 38-47) and the client key acts as a command, and storage providers are called by the storage server to securely store and retrieve data items (col. 7, lines 54-60).

As per claim 36:

Further, Thomlinson teaches an item authentication code is generated using a MAC in conjunction with a randomly generated item authentication key (col. 11, lines 30-36).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 12 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomlinson et al., United States Patent No. 6,044,155 as applied to claims 1 and 13 above, and further in view of Cisco Systems, 1992.

As per claim 12:

Further, Thomlinson fails to teach the network identity comprises a MAC address. Cisco Systems, Inc. teaches a MAC address accounting information for

Internet protocol traffic based on the source and destination MAC addresses on LAN interfaces.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Thomlinson by including a MAC address connected to the internet. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Cisco Systems, Inc., in order to allow the Internet destinations to be recorded and accounted appropriately.

As per claim 16:

Further, Thomlinson fails to teach the network identity comprises a MAC address. Cisco Systems, Inc. teaches a MAC address accounting information for Internet protocol traffic based on the source and destination MAC addresses on LAN interfaces.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Thomlinson by including a MAC address connected to the internet. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Cisco Systems, Inc., in order to allow the Internet destinations to be recorded and accounted appropriately.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Nadia Khoshnoodi
Examiner
Art Unit 2133
4/15/2005

NK

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100